PP 5/12/05
insert> This application claims priority from 60/144,066 filed 7/16/1999.

GLOBAL ENCRYPTION SYSTEM

DESCRIPTION

Field of the Invention

This invention relates generally to the field of data encryption and, more particularly, to a method and apparatus for encryption, transmission and decryption utilizing a broadcast random data sequence accessible by the sender and receiver.

Description of the Related Art

In recent years, several papers and patents have disclosed advances in developing information-theoretically secure cryptosystems. Where possible, information-theoretically secure systems have substantial advantages over cryptosystems based on assumptions of an adversary's processing power. Such computational systems include public key systems and some private key systems such as the Digital Encryption Standard (DES) and Advanced Encryption Standards (AES). One advantage of information-theoretically secure systems is security: information-theoretically secure systems implicitly assume that an adversary has unlimited computing power, so such cryptosystems are generally regarded as having achieved the "unbreakable" status of a one-time pad. In contrast, cryptosystems that base their security on an adversary's estimated processing power cannot achieve this status and so are less secure.